



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/803,434	03/18/2004	Robert Wilmer Rodenbeck	3054-74724	5439
27268	7590	08/09/2005	EXAMINER	
BAKER & DANIELS LLP 300 NORTH MERIDIAN STREET SUITE 2700 INDIANAPOLIS, IN 46204				BROWN, VERNAL U
		ART UNIT		PAPER NUMBER
				2635

DATE MAILED: 08/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/803,434	RODENBECK ET AL.
	Examiner Vernal U. Brown	Art Unit 2635

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 19 May 2005.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-7,10-16 and 18-29 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-7,10-16 and 18-29 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

- Certified copies of the priority documents have been received.
- Certified copies of the priority documents have been received in Application No. _____.
- Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____

5) Notice of Informal Patent Application (PTO-152)

6) Other: _____

DETAILED ACTION

This action is responsive to communication filed on May 19, 2005.

Response to Amendment

The examiner has acknowledged the amendment of claims 1, the cancellation of claims 8-9, 17, and the addition of claims 27-29.

Response to Arguments

Applicant's arguments with respect to claims 1-7, 10-16 have been considered but are moot in view of the new ground(s) of rejection.

Regarding applicant argument regarding claim 18, Kniffin et al. teaches a central access control system (18) in which access information is stored (col. 2 lines 44-45), and a plurality of remote access control systems. The plurality of remote access system is evidenced by the user identifying the remote control system to the central access controller (clearinghouse) that the access is desired to (col. 2 lines 37-38).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 18, 24-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Kniffin et al. US Patent 6072402.

Regarding claim 18, Kniffin et al. teaches a security control system configured to control the locking and locking of doors in a facility (col. 2 lines 25-30) the wireless security control system comprising a central access control system (18) in which access information is stored (col. 2 lines 44-45), and a plurality of remote access control systems (plurality of access control system is implied by the user identifying the access system the user desires to access, col. 2 lines 37-38) each being adapted to be mounted to a respective one of the doors of the facility to control the locking and unlocking of the respective door (col. 2 lines 25-31), the central access control system wirelessly transmitting access information to the plurality of remote access control systems (col. 5 lines 42-47).

Regarding claim 24, Kniffin et al. teaches the central wireless communicator communicates with more than one remote access control system (col. 7 lines 20-25).

Regarding claims 25-26, Kniffin et al. teaches each of the remote access control systems further includes a reader (28) electrically coupled to the remote access controller and adapted to read user data and each of the remote access control systems periodically transmits the associated user data to the central access controller (col. 4 lines 54-56).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 2, 4, 10-12, 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kniffin et al. US Patent 6072402 in view of Pinzon US Patent 6161005.

Regarding claim 1, Kniffin et al. teaches a wireless security control system (figure 1) for use in a facility having a plurality of doors (col. 5 lines 40-44), the wireless security control system comprising a central access control system (18) in which access information is stored (col. 2 lines 44-45), and a plurality of remote access control systems each being adapted to be mounted to a respective one of the doors of the facility to control the locking and unlocking of the respective door (col. 2 lines 25-31), the central access control system wirelessly transmitting access information to the plurality of remote access control systems prior to any users associated with the access information making any attempts to unlock any of the doors (col. 5 lines 42-47), each of the remote access control systems being configured to receive wirelessly and store at least some of the access information from the central access control system (col. 5 lines 53-55), each of the remote access control systems being configured to control the locking and unlocking of the respective door using the access information stored therein, each of the plurality of remote access control systems making a decision whether to unlock the respective door in response to a user making an attempt to unlock the door based on the access information stored therein and

without having to further communicate with the central access control system (col. 5 lines 53-57). Kniffin et al. is however silent on teaching access information is transmitted to the access control system independent of independent of any user making a request to unlock the door. Pinzon in an art related door unlocking system teaches pre-programming the access code into a locking unit (col. 6 lines 32-41) in order to change and update the access codes.

It would have been obvious to one of ordinary skill in the art for access information is transmitted to the access control system independent of independent of any user making a request to unlock the door in Kniffin et al. as evidenced by Pinzon because Kniffin et al. suggest programming the locking mechanism with the access code when access is requested and Pinzon teaches pre-programming the access code into a locking unit in order to change and update the access codes.

Regarding claim 2, Kniffin et al. teaches the remote access control systems includes an antenna, an access controller, and a receiver that is electrically coupled to the antenna and that communicates the wireless information received by the antenna to the access controller (figure 1).

Regarding claim 4, Kniffin et al. teaches the remote access control systems is further adapted to transmit wireless information to the central access control system (col. 4 lines 54-56).

Regarding claim 10, Kniffin teaches a remote access control system (figure 1) adapted to be mounted to a door to control the locking and unlocking of the door and adapted to receive wireless information from a central access control system located remotely from the access control system (col. 2 lines 31-40), the remote access control system comprising: a reader (proximity detector) adapted to read user data presented to reader (col. 3 lines 56-58);

a remote wireless communicator adapted to receive wireless information from the central access control system, the wireless information being transmitted to the remote wireless communicator where it is stored prior to a user making an attempt to unlock the door (col. 2 lines 44-53); a remote access controller electrically coupled to the remote wireless communicator and configured to receive the information from the remote wireless communicator, the remote access controller being configured to control the locking and unlocking of the door using the stored wireless information, the remote access controller making a decision from the previously stored wireless information and without requiring additional information from the central access control system about whether to unlock the door in response to the user making the attempt to unlock the door (col. 4 line 52-col. 5 line 2). Kniffin et al. further teaches providing user-updated information to the remote access controller (col. 5 lines 52-55).

Regarding claim 11, Kniffin et al. teaches the remote access control systems further comprises a battery coupled to the respective reader, the respective remote access controller, and the respective remote wireless communicator (col. 4 lines 53-55, figure 1).

Regarding claim 12, Kniffin et al. teaches the user data is stored on tokens (col. 3 lines 50-58), each of the remote access control systems is adapted to store user history information regarding which tokens were granted access (col. 4 lines 52-53), and each of the remote access control systems is configured to transmit the user history information to the central access control system (col. 4 lines 54-56).

Regarding claim 24, Kniffin et al. teaches the central wireless communicator communicates with more than one remote access control system (col. 7 lines 20-25).

Regarding claims 25-26, Kniffin et al. teaches each of the remote access control systems

further includes a reader (28) electrically coupled to the remote access controller and adapted to read user data and each of the remote access control systems periodically transmits the associated user data to the central access controller (col. 4 lines 54-56).

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kniffin et al. U.S Patent 6072402 in view of Pinzon US Patent 6161005 and further in view of Goldman U.S Patent 5321963.

Regarding claim 3, Kniffin et al. teaches mounting a portion of the remote access control system on both side of the door (col. 5 lines 48-50) but is silent on teaching the remote access control system includes a housing having an inner portion mounted on the inside of the door and an outer portion mounted on the outside of the door. One skilled in the art recognizes that it is conventional practice to have an access control system in which an inner portion of the system is mounted on the inside and an outer portion mounted on the outside in order to allow the access control mechanism to be operated from both side of the door as further evidenced by Goldman (col. 1 lines 59-63). One skilled in the art further recognizes that an antenna is sometimes mounted on the outer portion of a housing as evidenced by communication units such as mobile and cellular phones and other communication devices.

It would have been obvious to one of ordinary skill in the art for the remote access control system to include a housing having an inner portion mounted on the inside of the door and an outer portion mounted on the outside of the door in Kniffin et al. in view of Pinzon as evidenced by Goldman because Kniffin et al. in view of Pinzon suggests a remote access control system controlling a door and one skilled in the art recognizes that it is conventional practice to

have an access control system in which an inner portion of the system is mounted on the inside and an outer portion mounted on the outside in order to allow the access control mechanism to be operated from both side of the door as further evidenced by Goldman. One skilled in the art further recognizes that an antenna is sometimes mounted on the outer portion of a housing as evidenced by communication units such as mobile and cellular phones.

Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kniffin et al. U.S Patent 6072402 in view of Pinzon US Patent 6161005 and further in view of Pilney et al. U.S Patent 5298883.

Regarding claim 5, Kniffin et al. teaches a remote access control system having a transmitter (42) and receiver (14) but is however silent on teaching the remote wireless communicator includes a switch for selectively choosing between receiving and transmitting the wireless information. Pilney et al. in an art related invention in the same field of endeavor of wireless system teaches a wireless communicator with a switch for selectively choosing between receiving and transmitting the wireless information (col. 2 lines 20-25).

It would have been obvious to one of ordinary skill in the art for the communicator transmits wireless information to the central access control system and the remote wireless communicator includes a switch for selectively choosing between receiving and transmitting the wireless receiver in Kniffin et al. in view of Pinzon as evidenced by Pilney et al. because Kniffin et al. in view of Pinzon suggests a wireless communicator for receiving and transmitting wireless information and Pilney et al. teaches a wireless transceiver with a transmit/receive switch for

selectively choosing between receiving and transmitting the wireless information and the remote wireless communicator transmitting information to the central access control system provides information to the central controller concerning the status of the lock.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kniffin et al. U.S Patent 6072402 in view of Pinzon US Patent 6161005 and further in view of Denison et al. U.S Patent 6359547.

Regarding claim 6, Kniffin et al. in view of Pinzon teaches providing updated information wirelessly to the remote access control system (col. 5 lines 52-55) but is silent on teaching the remote access control system includes a local communication port electrically coupled to the remote access controllers and adapted to provide wired communication from a portal device. Denison et al. in an art related Electronic Access Control Device invention teaches a remote access control system that includes a local communication port (col. 3 lines 36-39) as an alternative to the wireless communication means used by Kniffin et al..

It would have been obvious to one of ordinary skill in the art for the remote access control system includes a local communication port electrically coupled to the remote access controllers and adapted to provide wired communication from a portal device in Kniffin et al. in view of Pinzon as evidenced by Denison et al. because Kniffin et al. in view of Pinzon suggests transmitting information to the remote access control system and Denison et al. teaches a remote access control system that includes a local communication port for providing updates.

Claims 7, 13-17, 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kniffin et al. U.S Patent 6072402 in view of MacLellan et al. U.S Patent 6177861.

Regarding claims 7, 13, and 22 Kniffin et al. teaches providing user-updated information to the remote access controller (col. 5 lines 52-55) and the transfer of data is initiated by the user (col. 2 lines 31-34, col. 2 lines 44-46) but is silent on teaching the remote access control system periodically initiates wireless communication with the central access control system. MacLellan et al. in an art related communication system teaches remote unit transmitting status updates to the central controller (col. 3 lines 45-67). The transmission of the remote unit further initiate a transmission from the central control unit in the form of an acknowledgement (col. 5 lines 44-48) in order to ensure that data is transmitted when the remote unit is ready to accept data.

It would have been obvious to one of ordinary skill in the art for the remote access control system to periodically initiate the transmission of user updates to the remote access unit in Kniffin et al. as evidenced by MacLellan et al. because Kniffin et al. suggests transmitting user updates to the remote access unit and MacLellan et al. teaches the use of the remote unit to initiate communication with a central control unit to ensure that data is transmitted when the remote unit is ready to accept data.

Regarding claims 14 and 17, Kniffin et al. teaches a central access controller (20) and a central wireless communicator (26) connected to the central access controller (figure 1). Kniffin et al. further teaches a RF transmission system that include a paging system or a cellular system for transmitting control signal to the remote access unit (col. 2 lines 47-50) but is silent not explicit in teaching a plurality of central wireless communicators connected to the central controller. MacLellan et al. in an art related security system teaches a plurality of central wireless

communicators (103) connected to the central controller (figure 1) in order to limit the number of remote unit communicating with each central wireless communicators for avoiding interference.

It would have been obvious to one of ordinary skill in the art to have a plurality of central wireless communicators connected to the central controller in Kniffin et al. as evidenced by MacLellan et al. because Kniffin et al. teaches a central access controller and a central wireless communicator connected to the central access controller and MacLellan et al. teaches a plurality of central wireless communicators connected to the central controller in order to limit the number of remote unit communicating with each central wireless communicators for avoiding interference.

Regarding claim 15, Kniffin et al. teaches the central wireless communicator (26) communicating wirelessly with a remote access system (12) as shown in figure 1.

Regarding claim 16, Kniffin et al. teaches the central wireless communicator communicates with more than one remote access control system (col. 7 lines 20-25). Regarding claims 19-20, Kniffin et al. teaches a security system in which the central controller (20) is connected to the central access communicator (26) by a wired connection (figure 1) but is silent on teaching the central access controller is electrically coupled to the plurality of central access communicators by the bus. MacLellan et al. in an art related security system teaches central access controller is electrically coupled to the plurality of central access communicators by the bus (figure 1) and the bus is further controlled by network protocol (col. 2 lines 54-64) in order to provide a standard communication interface.

It would have been obvious to one of ordinary skill in the art for the central access controller is electrically coupled to the plurality of central access communicators by the bus in Kniffin et al. as evidenced by MacLellan et al. because Kniffin et al. suggests a security system in which the central controller is connected to the central access communicator by a wired connection and MacLellan et al. teaches central access controller is electrically coupled to the plurality of central access communicators by the bus and the bus is further controlled by network protocol in order to provide a standard communication interface.

Regarding claims 21 and 23, Kniffin et al. teaches a central access controller (20) and a central wireless communicator (26) connected to the central access controller (figure 1). Kniffin et al. further teaches a RF transmission system that include a paging system or a cellular system for transmitting control signal to the remote access unit (col. 2 lines 47-50). Kniffin et al. is however silent on teaching the central access controller communicate with central access communicators using RF technology. MacLellan et al. the central access controller communicating wirelessly with the central wireless communicators using RF technology (figure 1, col. 4 lines 2-5) as a low cost wireless communication system.

It would have been obvious to one of ordinary skill in the art for the central access controller communicating wirelessly with the central wireless communicators using RF technology in Kniffin et al. as evidenced by MacLellan et al. because Kniffin et suggests a central access controller and a central wireless communicator connected to the central access controller and MacLellan et al. teaches the central access controller communicating wirelessly with the central wireless communicators using RF technology as a low cost wireless communication means.

Claims 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kniffin et al. U.S Patent 6072402 in view of MacLellan et al. U.S Patent 6177861.

Regarding claims 19-20, Kniffin et al. teaches a security system in which the central controller (20) is connected to the central access communicator (26) by a wired connection (figure 1) but is silent on teaching the central access controller is electrically coupled to the plurality of central access communicators by the bus. MacLellan et al. in an art related security system teaches central access controller is electrically coupled to the plurality of central access communicators by the bus (figure 1) and the bus is further controlled by network protocol (col. 2 lines 54-64) in order to provide a standard communication interface.

It would have been obvious to one of ordinary skill in the art for the central access controller is electrically coupled to the plurality of central access communicators by the bus in Kniffin et al. as evidenced by MacLellan et al. because Kniffin et al. suggests a security system in which the central controller is connected to the central access communicator by a wired connection and MacLellan et al. teaches central access controller is electrically coupled to the plurality of central access communicators by the bus and the bus is further controlled by network protocol in order to provide a standard communication interface.

Regarding claims 21 and 23, Kniffin et al. teaches a central access controller (20) and a central wireless communicator (26) connected to the central access controller (figure 1). Kniffin et al. further teaches a RF transmission system that include a paging system or a cellular system for transmitting control signal to the remote access unit (col. 2 lines 47-50). Kniffin et al. is however silent on teaching the central access controller communicate with central access communicators using RF technology. MacLellan et al. the central access controller

communicating wirelessly with the central wireless communicators using RF technology (figure 1, col. 4 lines 2-5) as a low cost wireless communication system.

It would have been obvious to one of ordinary skill in the art for the central access controller communicating wirelessly with the central wireless communicators using RF technology in Kniffin et al. as evidenced by MacLellan et al. because Kniffin et al. suggests a central access controller and a central wireless communicator connected to the central access controller and MacLellan et al. teaches the central access controller communicating wirelessly with the central wireless communicators using RF technology as a low cost wireless communication means.

Claim 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kniffin et al. U.S Patent 6072402 in view of Pilney et al. US Patent 5298883.

Regarding claim 27, Kniffin et al. teaches the remote access control system receives access information from the central access communicator (clearing house) (col. 5 lines 42-47) but is silent on teaching the wireless communication is normally powered down. Pilney et al. in an art related communication system teaches a wireless communicator that is powered down when not in use (col. 3 lines 7-15) in order to conserve on the power supply.

It would have been obvious to one of ordinary skill in the art for the wireless communication device to be normally powered down in Kniffin et al. as evidenced by Pilney because Kniffin et al. suggests the remote access control system receives access information from the central access communicator and Pilney teaches a wireless communicator that is powered down when not in use in order to conserve on the power supply.

Regarding claims 28-29, Kniffin et al. teaches a security control system configured to control the locking and locking of doors in a facility (col. 2 lines 25-30) the wireless security control system comprising a central access control system (18) in which access information is stored (col. 2 lines 44-45), and a plurality of remote access control systems (plurality of access control system is implied by the user identifying the access system the user desires to access, col. 2 lines 37-38) each being adapted to be mounted to a respective one of the doors of the facility to control the locking and unlocking of the respective door (col. 2 lines 25-31), the central access control system wirelessly transmitting access information to the plurality of remote access control systems (col. 5 lines 42-47). Kniffin et al. is however silent on teaching the wireless communication is normally powered down. Pilney et al. in an art related communication system teaches a wireless communicator that is powered down when not in use (col. 3 lines 7-15) in order to conserver on the power supply.

It would have been obvious to one of ordinary skill in the art for the wireless communication device to be normally powered down in Kniffin et al. as evidenced by Pilney because Kniffin et al. suggests the remote access control system receives access information from the central access communicator and Pilney teaches a wireless communicator that is powered down when not in use in order to conserver on the power supply.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Vernal U. Brown whose telephone number is 571-272-3060. The examiner can normally be reached on 8:30-7:00 Monday-Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached on 571-272-3068. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Vernal Brown
August 2, 2005



BRIAN ZIMMERMAN
PRIMARY EXAMINER